RUHR-UNIVERSITÄT BOCHUM

RUB

Security Analysis of the Chrome Sandbox in Windows, Linux and macOS

hgi Lehrstuhl für Netz- und Datensicherheit

Stean

RUHR-UNIVERSITÄT BOCHUM

RUB

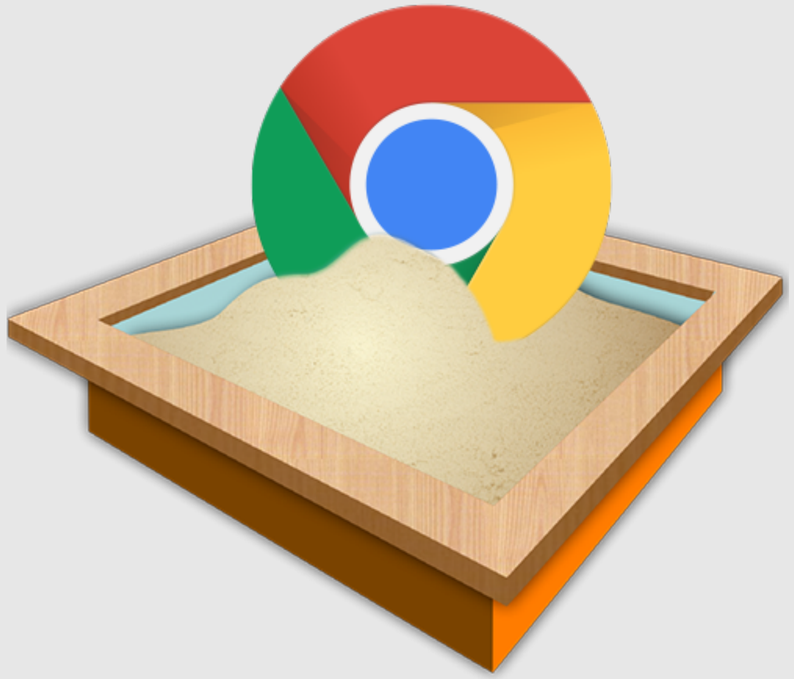
Wie sperre ich meine Kinder(-prozesse) sicher im (Chrome-)Sandkasten ein?

hgi Lehrstuhl für Netz- und Datensicherheit

Stean

Agenda

- Einleitung
- Chrome-Architektur
- Native Sandbox-Implementierungen
  - Windows 
  - Linux 
  - macOS 
- Angriffe



Einleitung

Definition einer Sandbox

- Sicherheitsmechanismus, der die möglichen Aktionen eines Programmes oder einer Softwarekomponente gemäß einer Richtlinie beschränkt [1]
- „*isolierter Bereich, in dem sich Software ausführen lässt, ohne dass diese auf die eigentliche Systemumgebung Zugriff hat*“ [2]
- Ziel: Verhinderung von Änderungen und unautorisiertem Zugriff auf das zugrunde liegende System

Einleitung

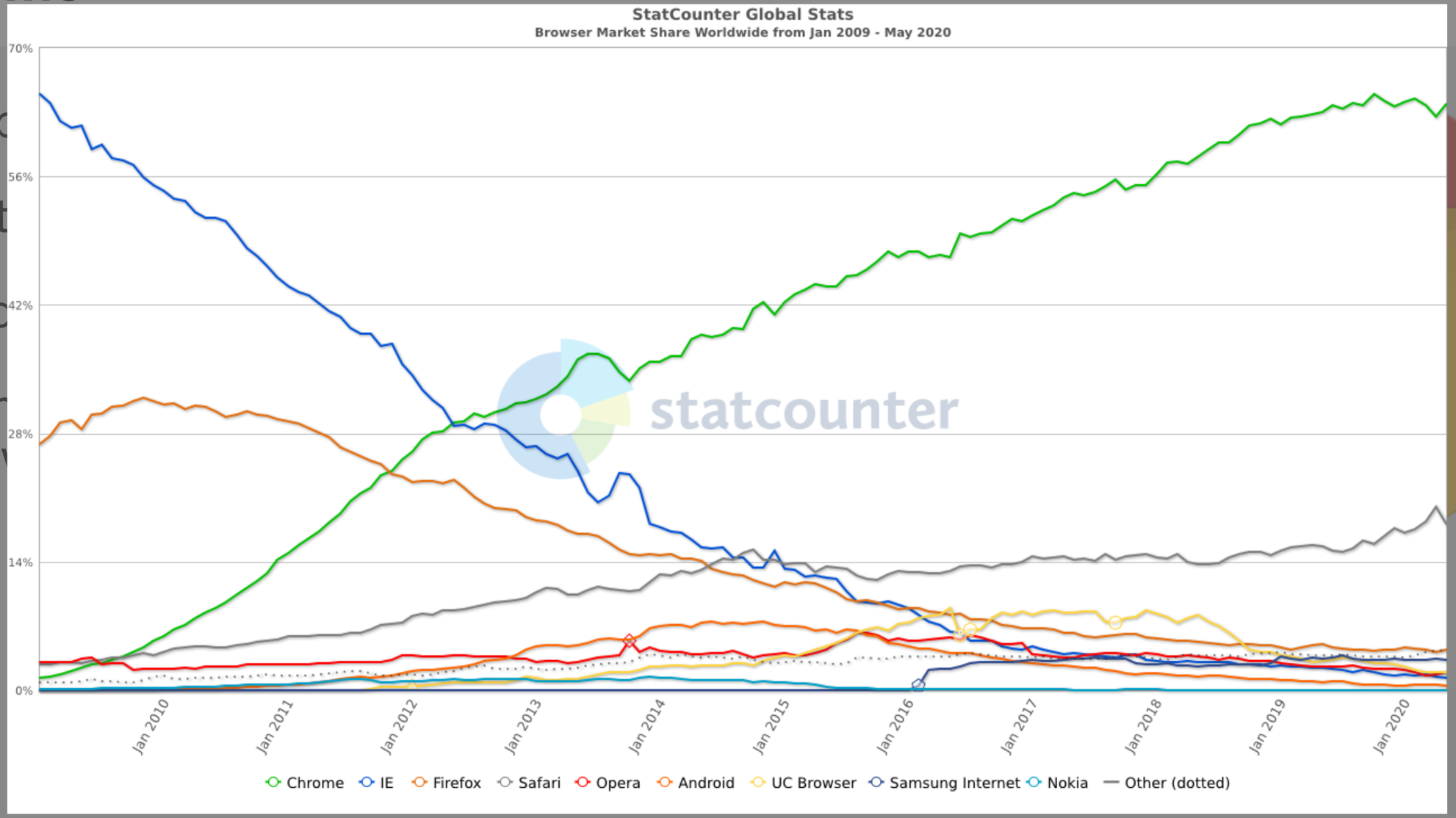
Chrome

- Webbrowser, der aktiv von Google entwickelt wird
- Erstes Release am 02.09.2008
- Code von Open Source Projekt „Chromium"
- Ist mit 65,89% (Mai 2020) einer der verbreitetsten Browser der Welt

Einleitung

Chrome

- Web
- Erst
- Coc
- Ist r
  Brov



Einleitung

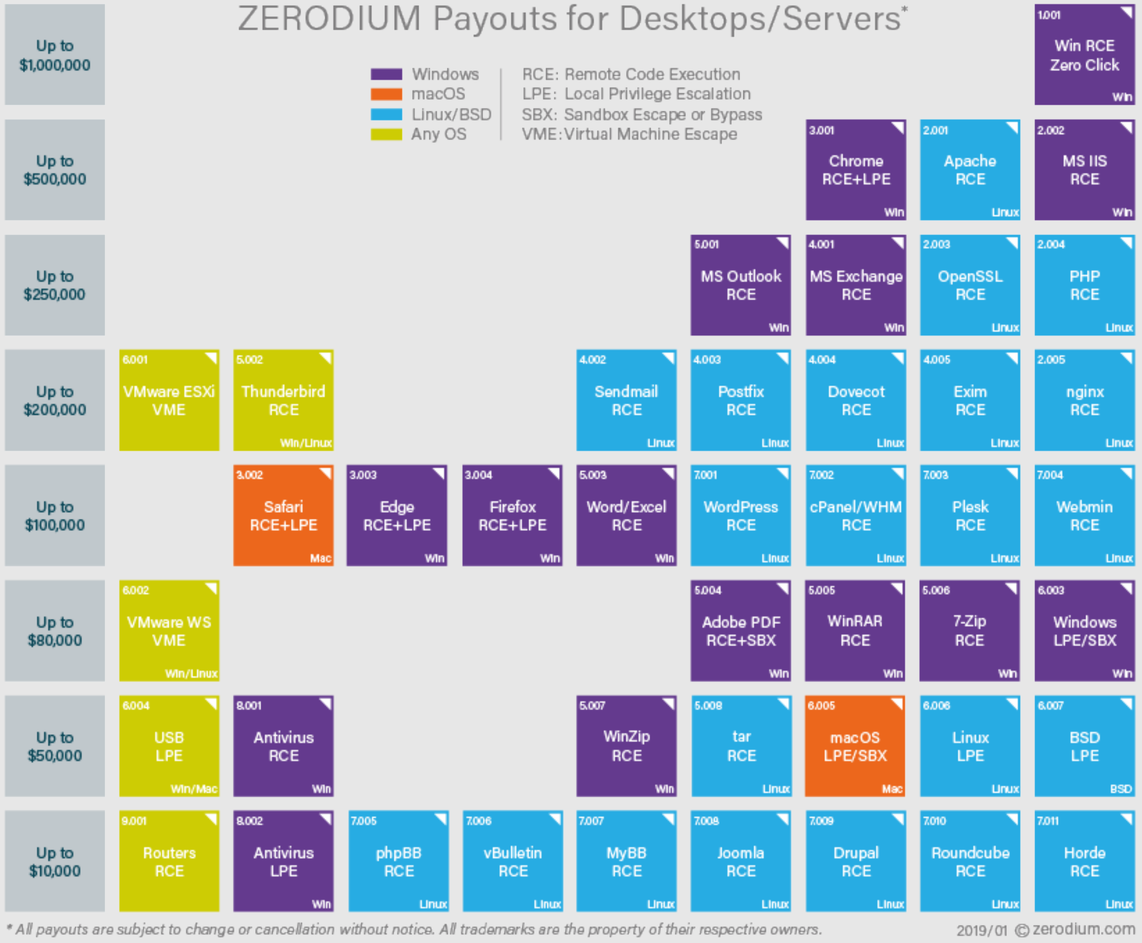
Geschichte der Sandbox

- Original Paper: *The Security Architecture of the Chromium Browser* (2008)
  - Security vs. Komplexität: Komplexität führt häufig zu Sicherheitslücken
  - Viele ausnutzbare Sicherheitslücken vor allem in der (relativ komplexen) Rendering Engine
  - Ergebnis: Sandbox ist ein effektiver Mechanismus, um die Auswirkungen ungepatchter Schwachstellen zu verringern
- Sandbox wurde in den letzten Jahren immer wieder auf die eigenen Securitymechanismen vieler Betriebsysteme angepasst

Einleitung

Motivation

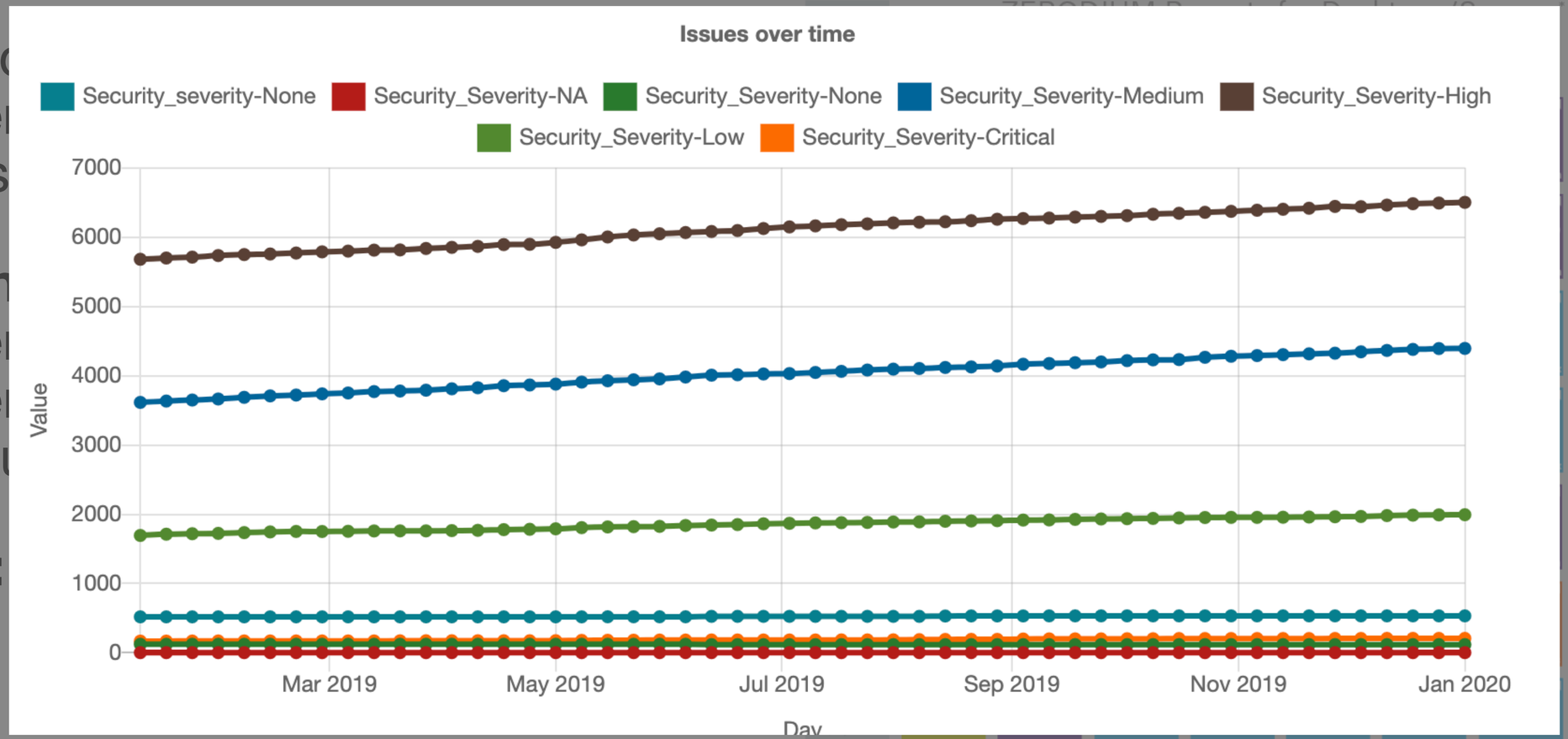
- Zero-day broker bieten für Chrome Sicherheitslücken teilweise sechsstellige Beträge
- **Erkenntnis:** Auch trotz allen Sicherheitsmaßnahmen ist eine Systemkompromittierung heutzutage möglich
- **Aber:** Es ist deutlich schwieriger



Einleitung

Motivation

- Zero-d
  Sicher
  sechs
- **Erken**
  Sicher
  Syste
  heutzu
- **Aber:**

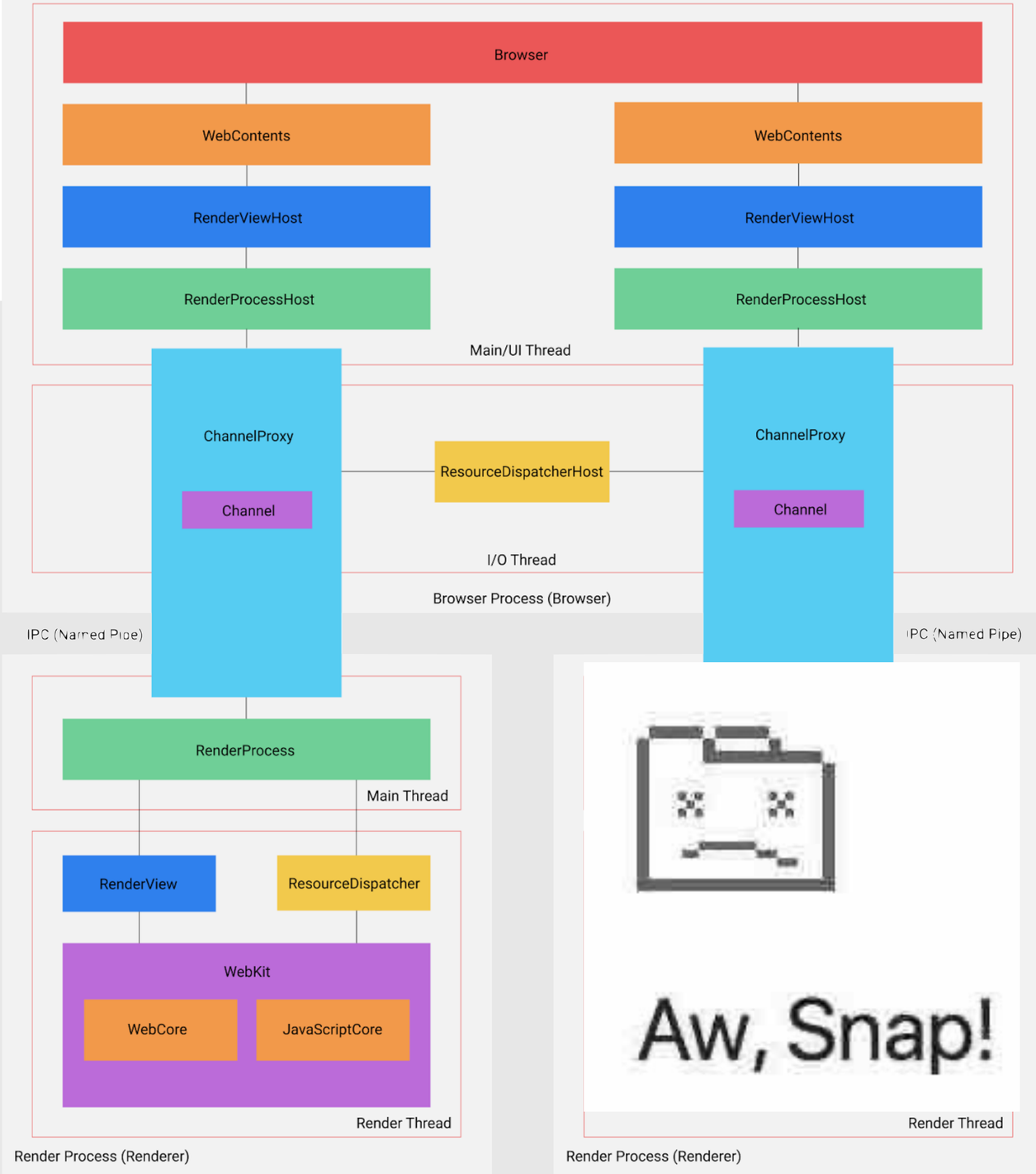


Chrome-Architektur

- Multi-Prozess Architektur
  - Aus Sicherheits-, Stabilitäts- und Geschwindigkeitsgründen
  - Einen Hauptprozess („Kernel“ oder „Broker“), der als uneingeschränkter Prozess läuft
  - Einen oder mehrere untergeordnete Helferprozesse
  - Mehrere Komponenten, von denen jede eine eigene Aufgabe und eigene Berechtigungen hat

Chrome-Architektur

- Multi-Prozess Architektur
  - Aus Sicherheits-, Stabilitäts- und Geschwindigkeitsgründen
  - Einen Hauptprozess („Kernel“ oder „Broker“), der als uneingeschränkter Prozess läuft
  - Einen oder mehrere untergeordnete Helferprozesse
  - Mehrere Komponenten, von denen jede eine eigene Aufgabe und eigene Berechtigungen hat



Sandbox-Implementierung

Windows - Sicherheitsmaßnahmen

- Job Objekte
- Integrity levels
- Alternative desktops
- Restricted Tokens
- Process wide mitigation policy
  - Address Space Layout Randomization (ASLR)
  - Control Flow Guard (CFG)
- Deaktivierung von Extension Points
- Heap Terminate
- Strict Handle Checks
- Win32k.sys lockdown
- Disable Font Loading
- Disable Image Load from Remote Devices
- Disable Image Load from low integrity level

Sandbox-Implementierung

Windows

- Job Objekt(e)
  - Bietet Gruppierung von mehreren Prozessen als eine Einheit
  - Operationen, die auf ein Job Objekt angewandt werden, betreffen alle Prozesse, die dem Objekt zugewiesen wurden
  - Ermöglicht Beschränkung von Systemressourcen (ähnlich ulimits unter Linux)
  - In der Chrome Sandbox vor allem in Verbindung mit der JOB_OBJECT_LIMIT_ACTIVE_PROCESS Beschränkung verwendet
    - Verhinderung, dass Sandbox-Prozesse Unterprozesse starten können

Sandbox-Implementierung

Windows

- Integritätsstufen (Integrity levels)
  - Implementiert seit Vista
  - Mandatory access control (MAC) Mechanismus
  - Objekten wie Prozessen und Dateien kann eine Integritätsstufe zugewiesen werden
  - Objekte mit einer höheren Stufe können auf niedrigere Stufen schreiben, aber niedrigere können nach oben hin nur lesen
  - Integritätsstufe des Elternprozesses wird standardmäßig vererbt
  - Im Falle der Chrome Sandbox werden gesandboxte Prozesse explizit mit der niedrigsten Stufe gestartet, damit diese so wenig Änderungen wie möglich vornehmen können

Sandbox-Implementierung

Windows

- Integritätsstufen (Integrity levels)
  - Implem
  - Mandat
  - Objekte werden
  - Objekte r niedrigere können
  - Integrit
  - Im Falle der Chrome Sandbox werden gesandboxte Prozesse explizit mit der niedrigsten Stufe gestartet, damit diese so wenig Änderungen wie möglich vornehmen können

SID	Name (Level)	Use
S-1-16-0x0	Untrusted (0)	Used by processes started by the Anonymous group. It blocks most write access.
S-1-16-0x1000	Low (1)	Used by Protected Mode Internet Explorer. It blocks write access to most objects (such as files and registry keys) on the system.
S-1-16-0x2000	Medium (2)	Used by normal applications being launched while UAC is enabled.
S-1-16-0x3000	High (3)	Used by administrative applications launched through elevation when UAC is enabled, or normal applications if UAC is disabled and the user is an administrator.
S-1-16-0x4000	System (4)	Used by services and other system-level applications (such as Wininit, Winlogon, Smss, and so forth).

Sandbox-Implementierung

Linux

- Basiert auf 2 Ebenen:
  - **"Semantische" Ebene**
    - Hindert Prozess daran, auf die meisten Systemressourcen zuzugreifen
    - Sandbox-Typen:
      - Setuid (SUID)
      - User namespaces
      - SELinux
      - AppArmor
  - **„Angriffsreduktions-“ Ebene**
    - Ziel: Angriffsfläche des Kernels verringern (z.B. durch Filtern der erlaubten Syscalls)
    - Sandbox-Typen:
      - Seccomp-bpf
      - Seccomp-legacy

Sandbox-Implementierung

macOS

- Chrome nutzt macOS systemeigener Sandbox-Technologie „Seatbelt“
- Seatbelt
  - Initialisierung über sandbox_init() Funktion
  - baut auf FreeBSD’s Mandatory Access Control Framework (MACF) auf
  - Realisiert als „Policy“-Kernelmodul unter `/System/Library/Extensions/Sandbox.kext`
  - Bei jedem entsprechenden Syscall wird Seatbelt konsultiert und gefragt, ob Zugriff gestattet werden kann

Sandbox-Implementierung

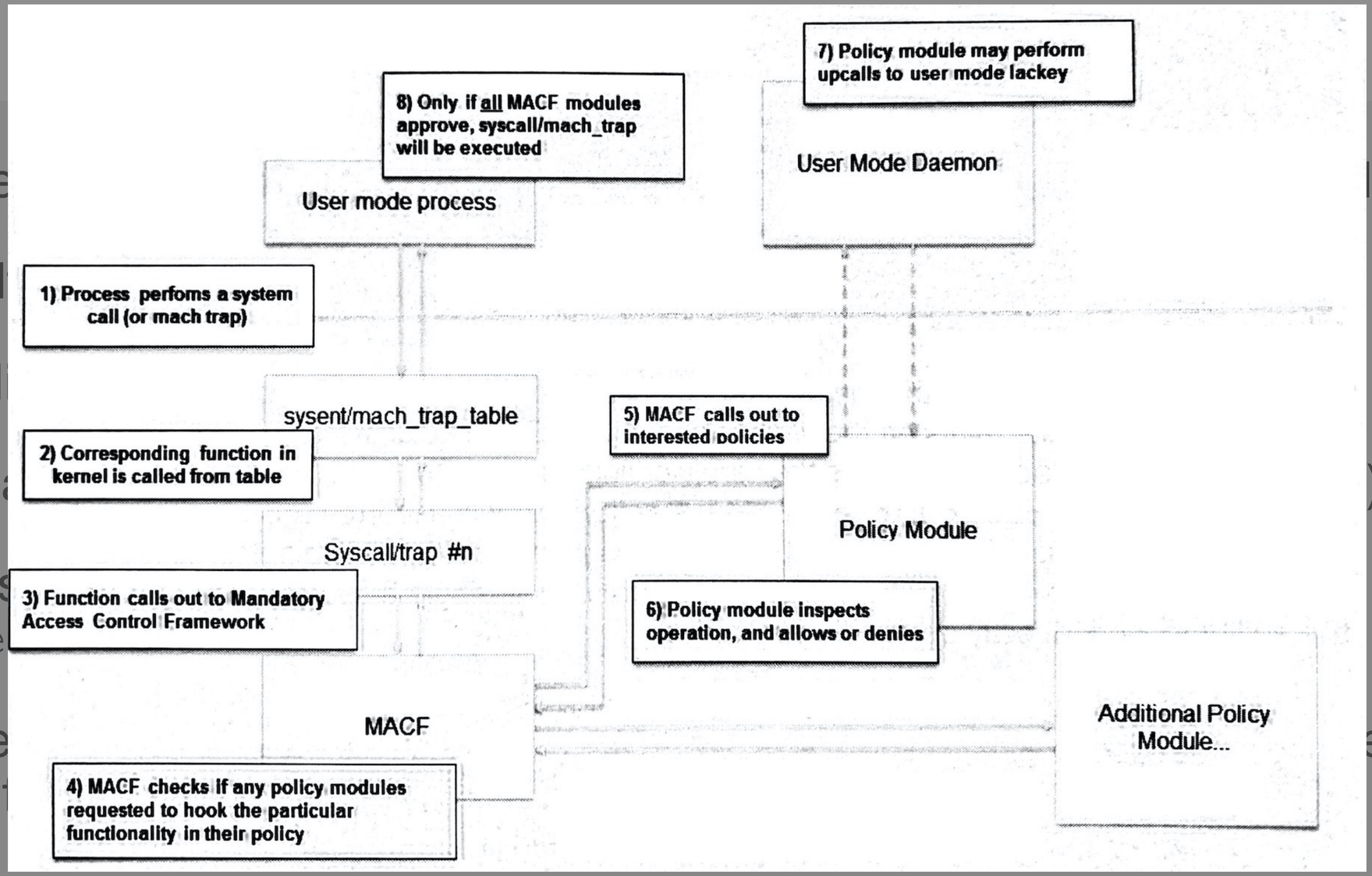
macOS

- Chrome
- Seatbel
  - Initial
  - baut a
  - Realis
    Exte
  - Bei je

lt“

) auf

efragt, ob
Zugrif



Sandbox-Implementierung

macOS

- Chrome nutzt macOS systemeigener Sandbox-Technologie „Seatbelt“
- Seatbelt
  - Initialisie
  - baut auf rk (MACF) auf
  - Realisier rary/ Extens
  - Bei jedem entsprechenden Syscall wird Seatbelt konsultiert und gefragt, ob Zugriff gestattet werden kann

```
; Sample SBPL Profile: Actions, operations,
; filters and modifiers highlighted

(version 1)
(deny default)
(allow device-microphone)
(allow file-read-data
    (subpath "/usr/bin")
    (regex “^.*\\.dylib$")
    (with report))
```

Angriffe

- Die meisten „Sandbox escapes“ umgehen nicht direkt die Sandbox-Restriktionen, die durch das OS erzwungen werden
- Stattdessen Ausnutzung von Schwachstellen in Broker-Prozess über IPC-Mechanismus

Angriffe

- Die meisten „S ndbox-Restriktionen,
- Stattdessen A ss über IPC-Mechanismus

Bug-ID	CVE	Type	Summary
1062091		MojoJS POC	UAF in InstalledAppProvider-Impl
1055393		HTML POC	UAF in Accessibility
1041406		HTML POC	UAF in Portals
1035399	CVE-2020-6385	Patch POC	Site Isolation Bypass in BlobURL
1031142		Full Chain Exploit	UAF in DesktopMedia, Logic Bug in Extensions (Site Isolation Bypass)
1027152	CVE-2019-13726	Patch POC	Heap Overflow in PasswordFormManager
1025067	CVE-2019-13725	MojoJS POC	UAF in BluetoothAdapter
1024121	CVE-2019-13723	MojoJS POC	UAF in WebBluetoothServiceImpl
1024116	CVE-2019-13724	MojoJS POC	OOB Access in WebBluetoothServiceImpl
1007194	CVE-2019-13765	WriteUp	UAF in MojoCdmProxyService
1005753	CVE-2019-13693	Patch POC	UAF in IndexedDB
925864	CVE-2019-5788	MojoJS POC	UAF in FileSystemOperationRunner

Angriffe

CVE-2018-17462

- Basiert auf HTML5 Application Cache
  - Ermöglicht offline Webapplikationen
  - Von „Service Worker“ Standard abgelöst
  - Angabe von Ressourcen, die vorgehalten werden müssen:

```
<html manifest=”hello.appcache”>
  …
  <img src=”kitties.jpg” /> …
</html>
```

A.html

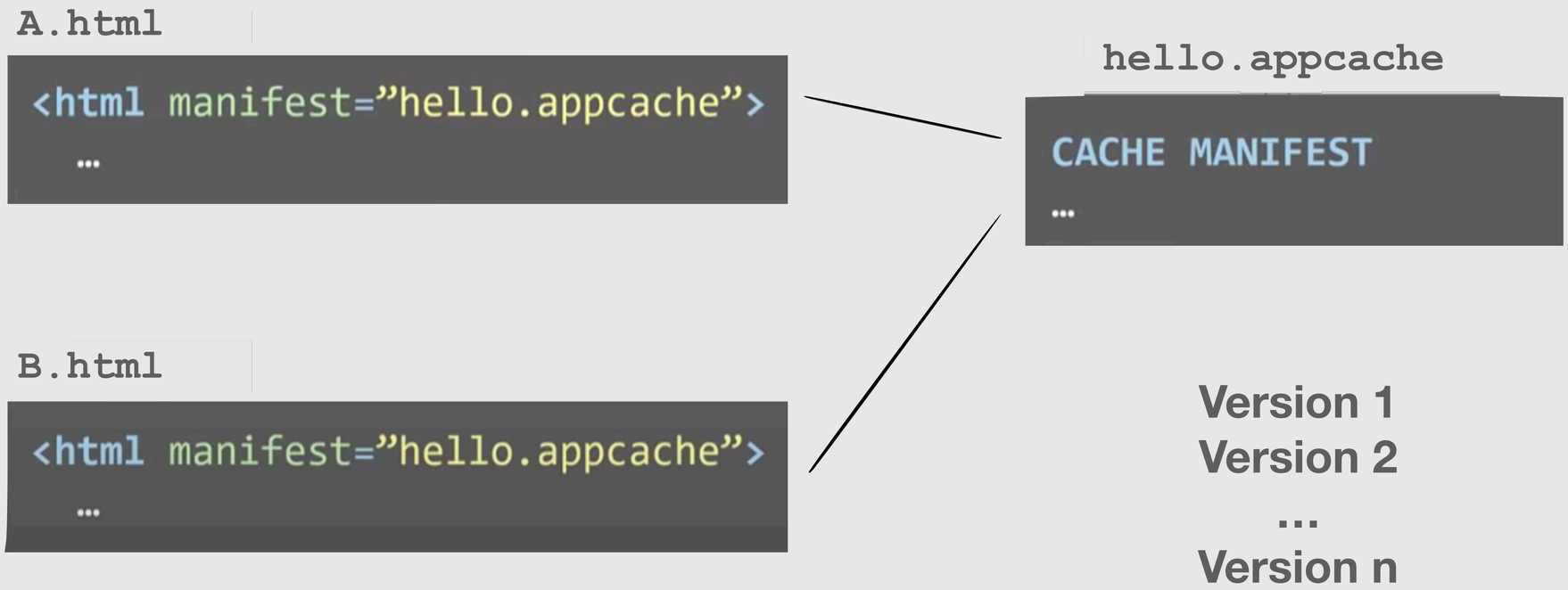
```
CACHE MANIFEST

CACHE:
kitties.jpg
…
```

hello.appcache

Angriffe

CVE-2018-17462

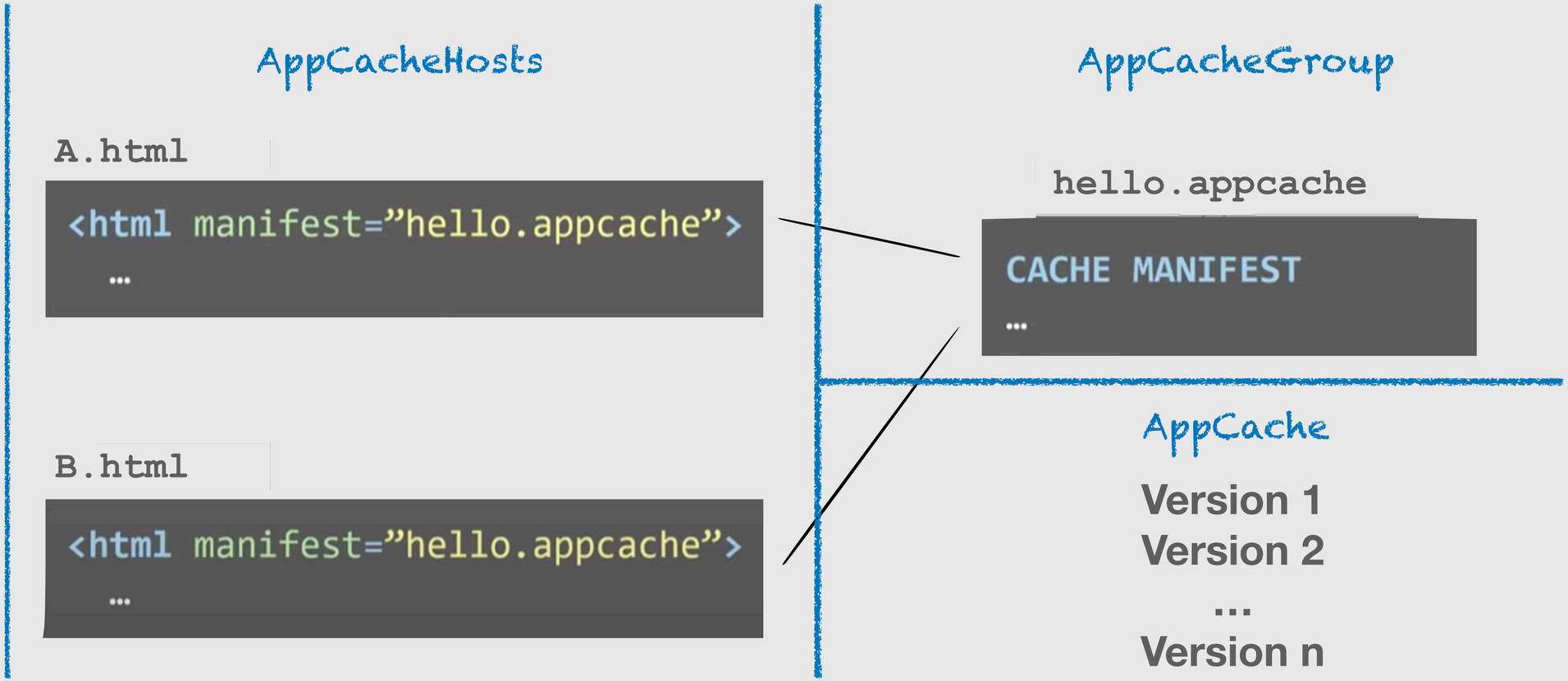
- AppCache Struktur:



Angriffe

CVE-2018-17462

- AppCache Struktur:



RUB

Angriffe

CVE-2018-17462

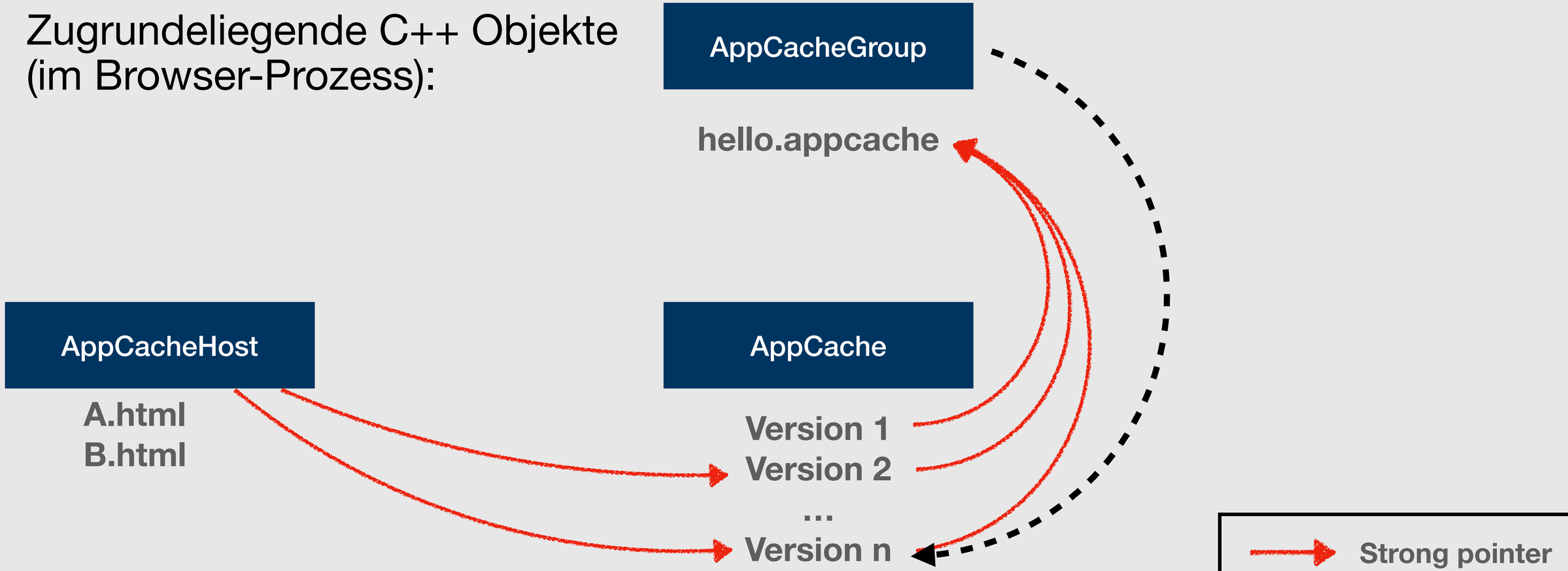
- IPC-Interface

```
// AppCache messages sent from the child process to the browser.
interface AppCacheBackend {
  RegisterHost(int32 host_id);
  UnregisterHost(int32 host_id);
  SetSpawningHostId(int32 host_id, int32 spawning_host_id);
  SelectCache(int32 host_id, Url document_url,
              int64 appcache_document_was_loaded_from,
              Url opt_manifest_url);
  SelectCacheForSharedWorker(int32 host_id, int64 appcache_id);
  MarkAsForeignEntry(int32 host_id,
                     Url document_url,
                     int64 appcache_document_was_loaded_from);
  [Sync] GetStatus(int32 host_id) => (AppCacheStatus status);
  [Sync] StartUpdate(int32 host_id) => (bool success);
  [Sync] SwapCache(int32 host_id) => (bool success);
  [Sync] GetResourceList(int32 host_id) => (array<AppCacheResourceInfo> resources);
};
```

Angriffe

CVE-2018-17462

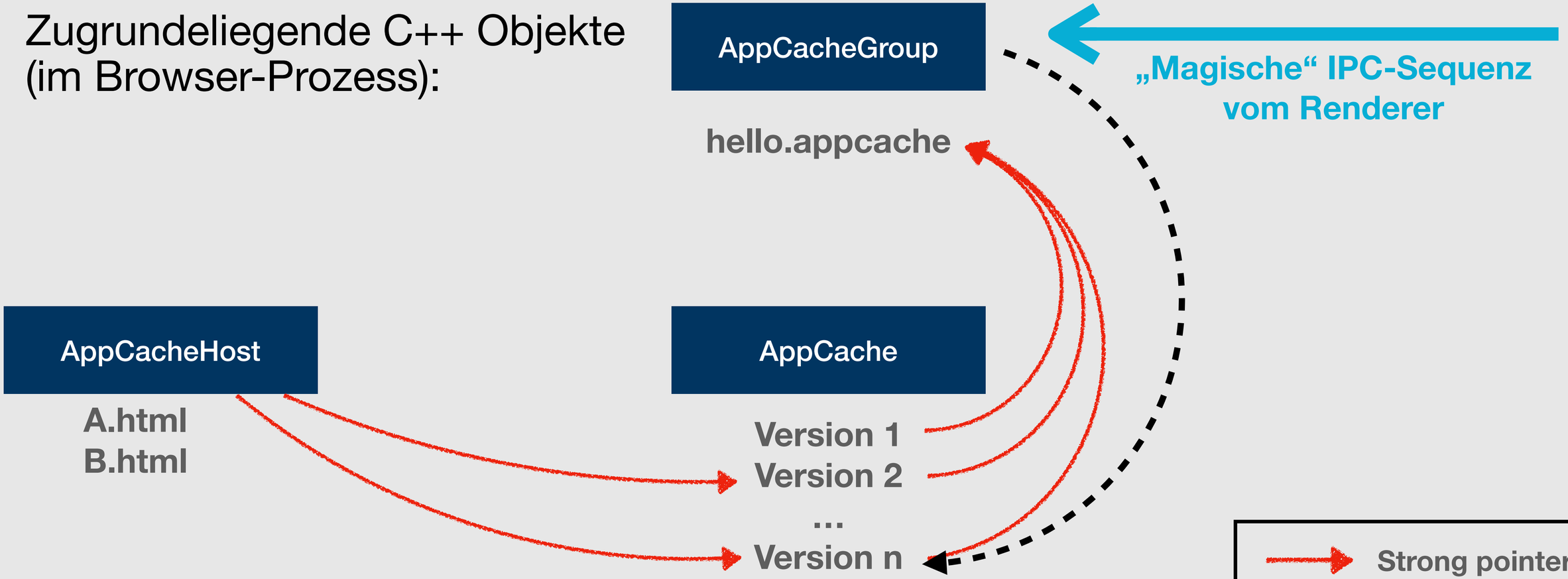
- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

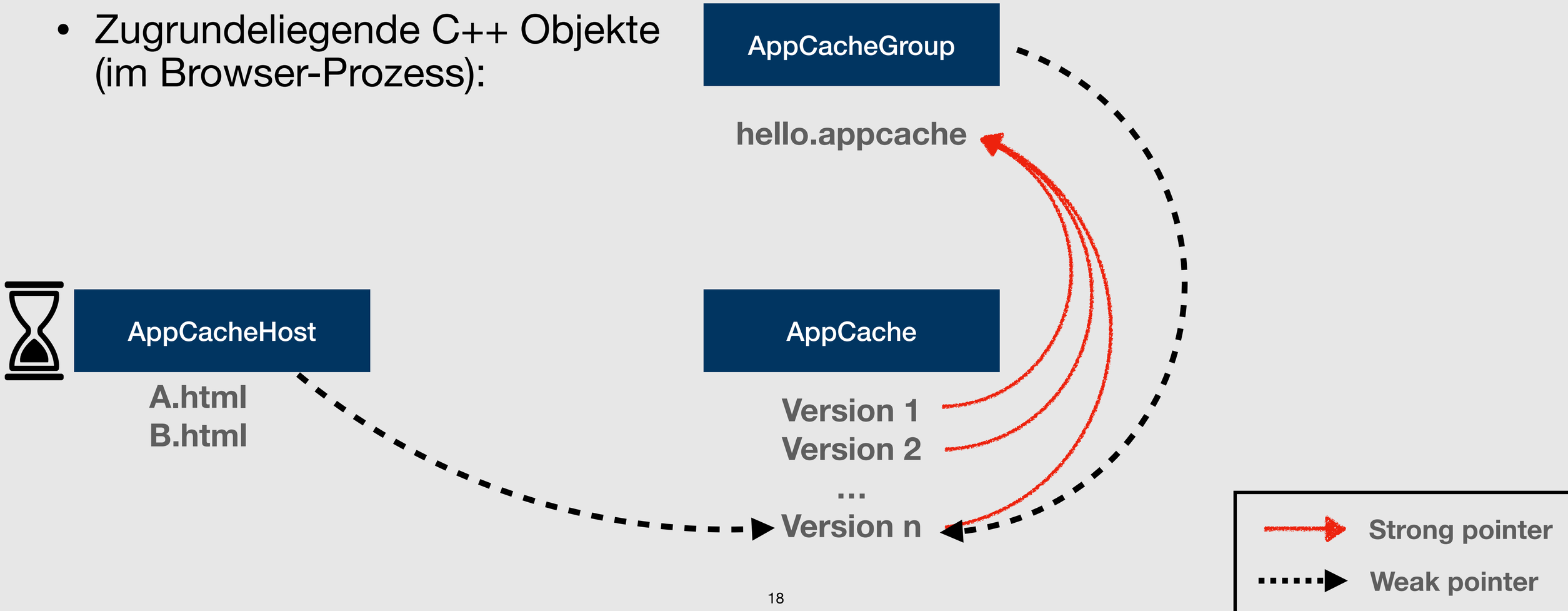
- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

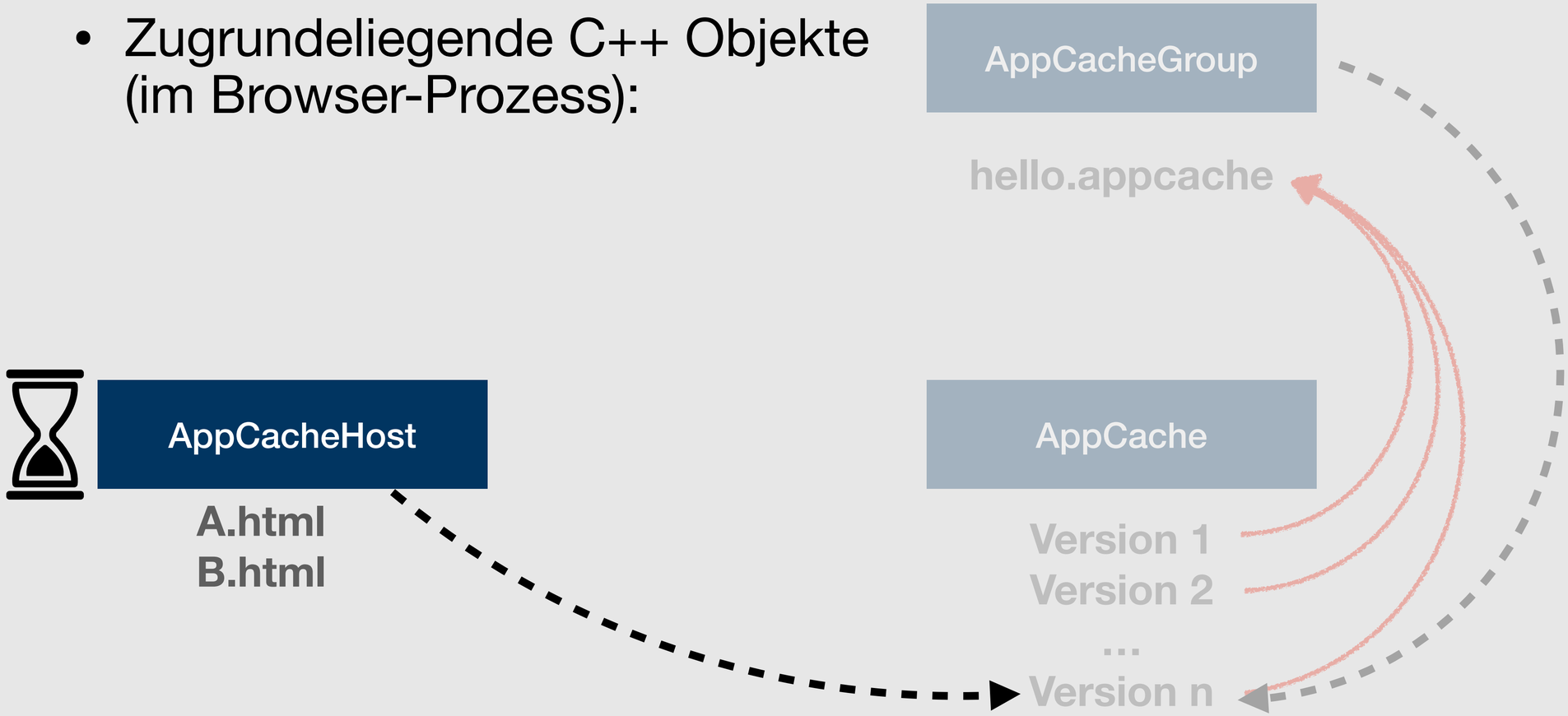
- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

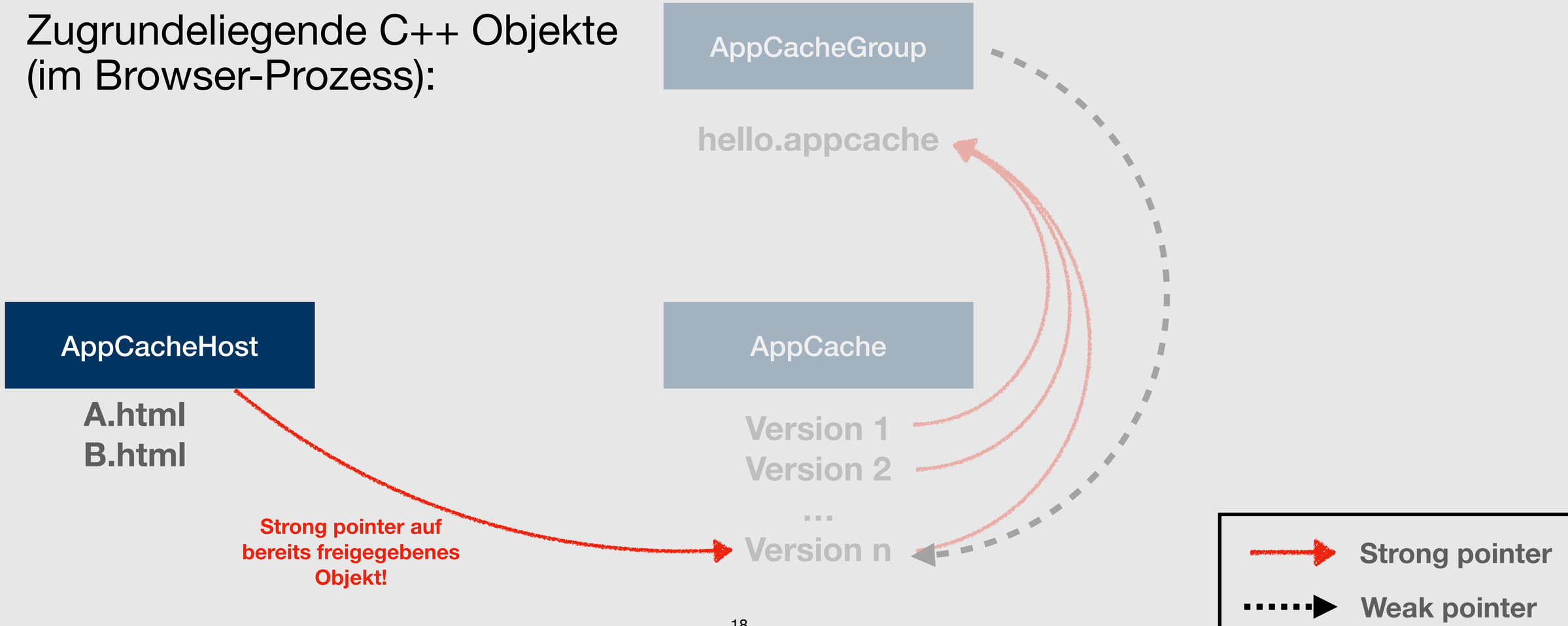
- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

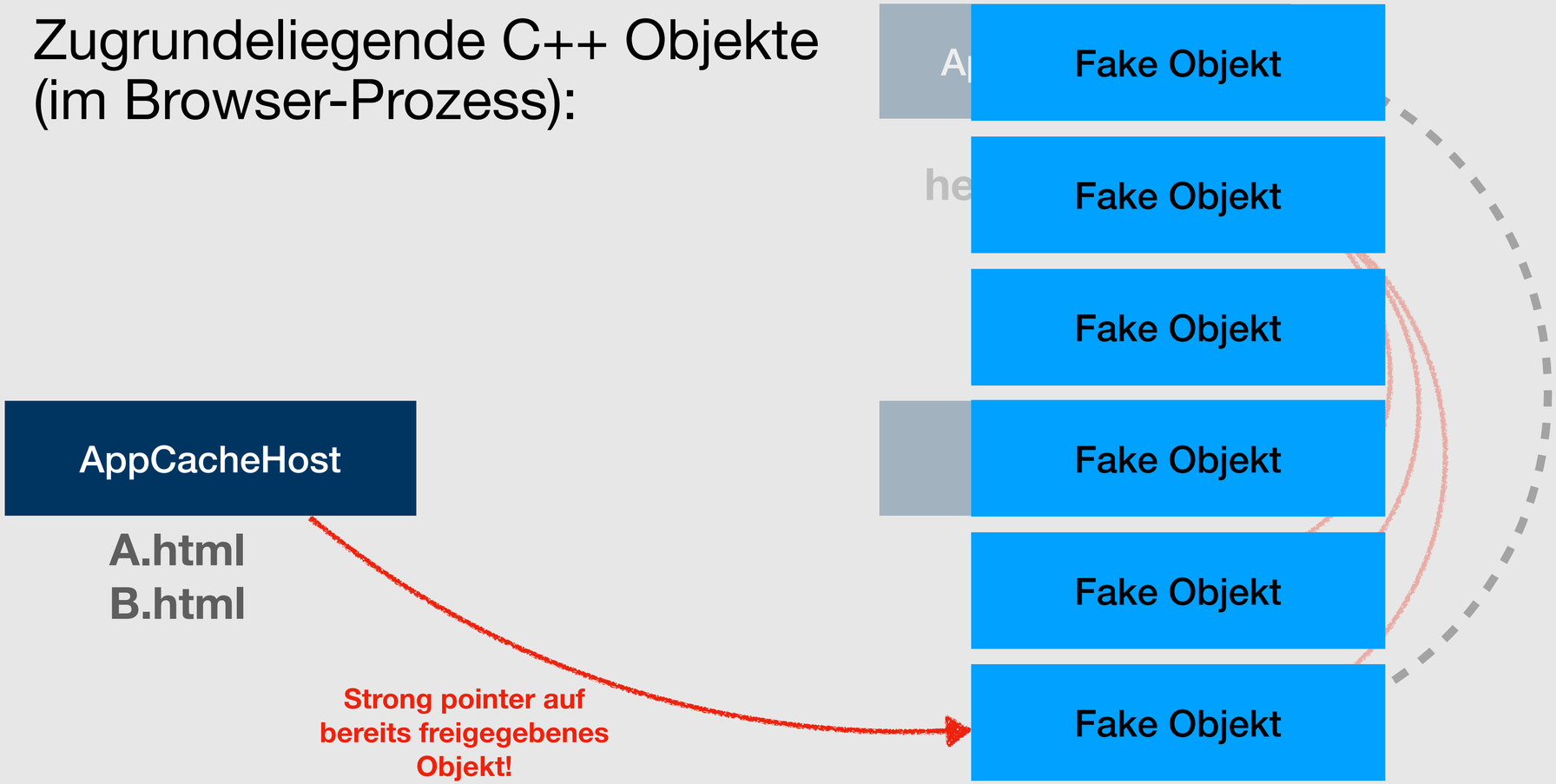
- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

- Zugrundeliegende C++ Objekte (im Browser-Prozess):



Angriffe

CVE-2018-17462

- Der Fix:

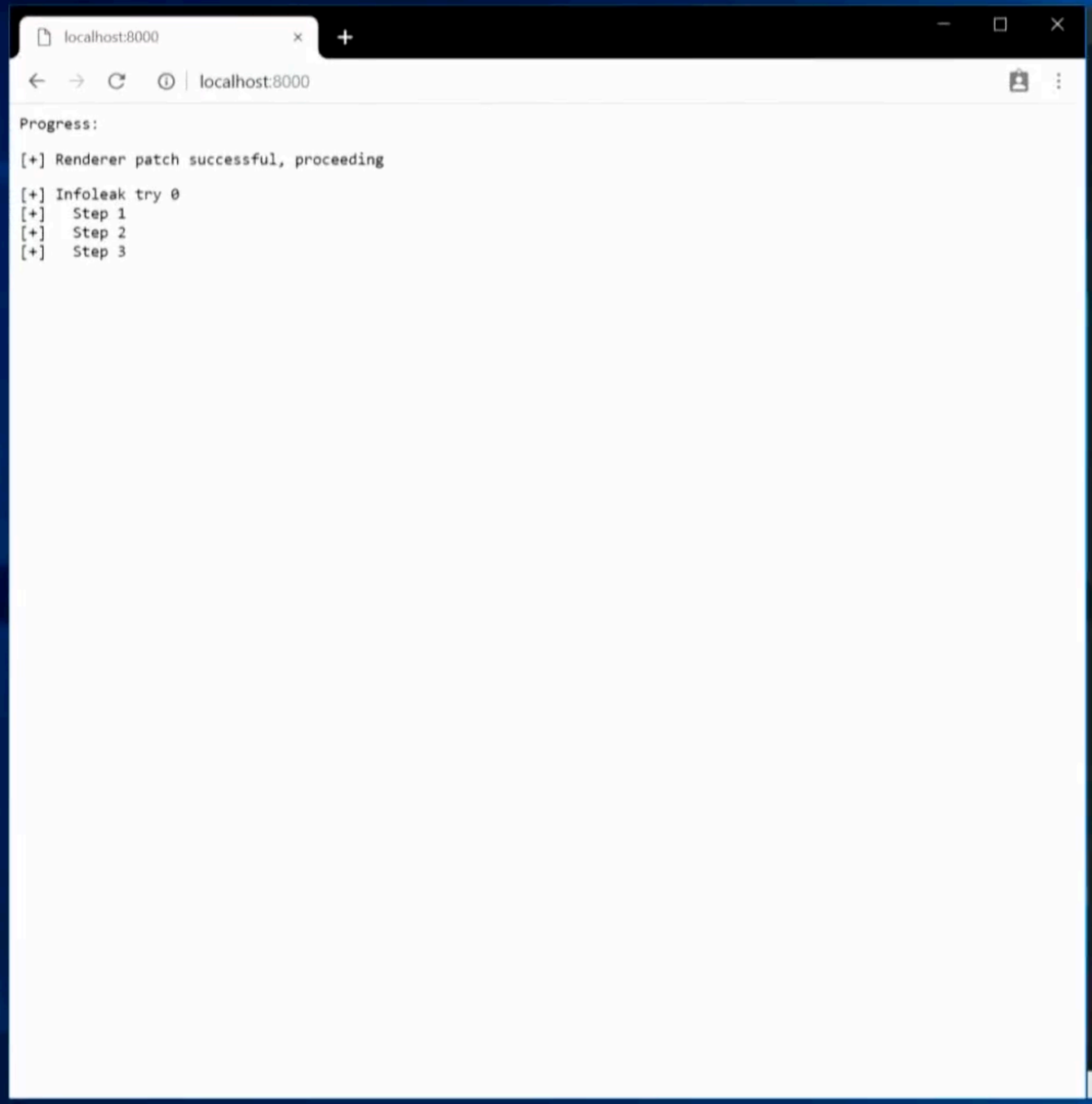
  content/browser/appcache/appcache_group.cc:

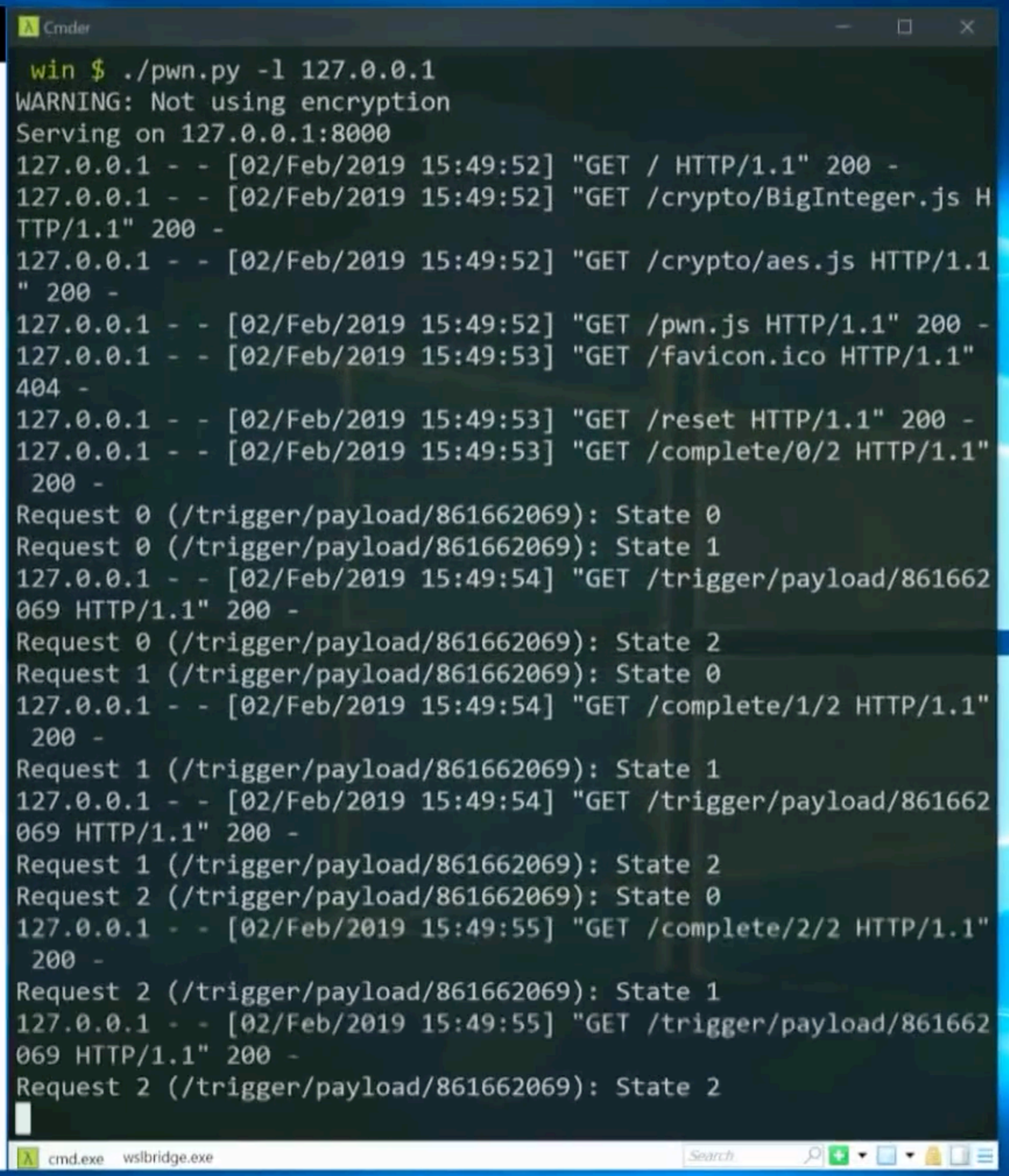
```
void AppCacheGroup::RemoveCache(AppCache* cache) {
  DCHECK(cache->associated_hosts().empty());
  if (cache == newest_complete_cache_) {
-   CancelUpdate();
    AppCache* tmp_cache = newest_complete_cache_;
    newest_complete_cache_ = nullptr;
+   CancelUpdate();
    tmp_cache->set_owning_group(nullptr);  // may cause this group to be deleted
  } else {
    scoped_refptr<AppCacheGroup> protect(this);
```

Angriffe

CVE-2018-17462

Demo


localhost:8000
localhost:8000
Progress:
[+] Renderer patch successful, proceeding
[+] Infoleak try 0
[+] Step 1
[+] Step 2
[+] Step 3


Cmder
win $ ./pwn.py -l 127.0.0.1
WARNING: Not using encryption
Serving on 127.0.0.1:8000
127.0.0.1 - - [02/Feb/2019 15:49:52] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [02/Feb/2019 15:49:52] "GET /crypto/BigInteger.js HTTP/1.1" 200 -
127.0.0.1 - - [02/Feb/2019 15:49:52] "GET /crypto/aes.js HTTP/1.1" 200 -
127.0.0.1 - - [02/Feb/2019 15:49:52] "GET /pwn.js HTTP/1.1" 200 -
127.0.0.1 - - [02/Feb/2019 15:49:53] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [02/Feb/2019 15:49:53] "GET /reset HTTP/1.1" 200 -
127.0.0.1 - - [02/Feb/2019 15:49:53] "GET /complete/0/2 HTTP/1.1" 200 -
Request 0 (/trigger/payload/861662069): State 0
Request 0 (/trigger/payload/861662069): State 1
127.0.0.1 - - [02/Feb/2019 15:49:54] "GET /trigger/payload/861662069 HTTP/1.1" 200 -
Request 0 (/trigger/payload/861662069): State 2
Request 1 (/trigger/payload/861662069): State 0
127.0.0.1 - - [02/Feb/2019 15:49:54] "GET /complete/1/2 HTTP/1.1" 200 -
Request 1 (/trigger/payload/861662069): State 1
127.0.0.1 - - [02/Feb/2019 15:49:54] "GET /trigger/payload/861662069 HTTP/1.1" 200 -
Request 1 (/trigger/payload/861662069): State 2
Request 2 (/trigger/payload/861662069): State 0
127.0.0.1 - - [02/Feb/2019 15:49:55] "GET /complete/2/2 HTTP/1.1" 200 -
Request 2 (/trigger/payload/861662069): State 1
127.0.0.1 - - [02/Feb/2019 15:49:55] "GET /trigger/payload/861662069 HTTP/1.1" 200 -
Request 2 (/trigger/payload/861662069): State 2
cmd.exe
wslbridge.exe
Search

Vielen Dank für Ihre Aufmerksamkeit!

Q&A

Fragen?

Quellen

Inhalte

- [0] https://gs.statcounter.com/browser-market-share#monthly-200901-202005
- [1] M. Bishop: Computer Security: Art and Science, book section 1440. Addison-Wesley Professional, 2nd ed., 2018.
- [2] https://www.security-insider.de/was-ist-eine-sandbox-a-740133/
- [3] https://web.archive.org/web/20161208060704/http://doeswhat.com/2008/09/02/it-was-when-not-if-google-chrome/
- [4] Barth et al.: The security architecture of the chromium browser, 2008
- [5] https://www.channelpartner.de/a/komplexitaet-ist-der-groesste-feind-von-sicherheit,3334011
- [6] https://www.heise.de/meinung/Komplexitaet-ist-der-Feind-der-Sicherheit-860711.html
- [7] https://www.computerworld.ch/business/interview/komplexitaet-feind-1728221.html
- [8] https://chromium.googlesource.com/chromium/src/+/master/docs/design/sandbox.md
- [9] https://blog.chromium.org/2008/09/multi-process-architecture.html
- [10] Russinovich et al.: Windows Internals Part 1 (6th Edition), 2012
- [11] https://chromium.googlesource.com/chromium/src/+/master/docs/linux/sandboxing.md
- J. Levin: *OS Internals - Volume III, vol. III. TechnoloGeeks, 2019, page 49
- https://www.youtube.com/watch?v=MMxtKq8UgwE

Quellen

Bilder

- Titelbild: https://unsplash.com/photos/z02yFSgVRbA (Photo by Markus Spiske on Unsplash)
- Windows-Logo: https://commons.wikimedia.org/wiki/File:Windows_logo_-_2012_derivative.svg
- Linux-Logo: https://www.iconfinder.com/icons/2993682/brand_brands_linux_logo_logos_icon
- Apple-Logo: https://commons.wikimedia.org/wiki/File:Apple-logo.png
- https://www.amazon.com/Executive-Sandbox-Day-at-Beach/dp/B0000A41ZO
- https://gs.statcounter.com/browser-market-share#monthly-200901-202005
- https://zerodium.com/program.html
- https://medium.com/@zicodeng/explore-the-magic-behind-google-chrome-c3563dbd2739
- https://bugs.chromium.org/p/chromium/issues/list?mode=chart&groupby=label&labelprefix=Security_Severity&start-date=2019-01-01&end-date=2019-12-31&can=1
- Russinovich et al.: Windows Internals Part 1 (6th Edition), 2012
- https://techcommunity.microsoft.com/t5/image/serverpage/image-id/90874i380E317CAEE266BC
- https://ubrigens.com/posts/sandbox_tour.html
- J. Levin: *OS Internals - Volume III, vol. III. TechnoloGeeks, 2019, page 49
- https://www.youtube.com/watch?v=MMxtKq8UgwE
- https://unsplash.com/photos/x4jRmkuDImo